(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 263 164 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
04.12.2002 Bulletin 2002/49

(51) Int Cl.7: **H04L 9/32**

(21) Application number: **01810637.7**

(22) Date of filing: **29.06.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **23.05.2001 EP 01810513**

(71) Applicant: **Büttiker, Daniel**
8400 Winterthur (CH)

(72) Inventor: **Büttiker, Daniel**
8400 Winterthur (CH)

(74) Representative: **Rutz, Peter**
RUTZ ISLER & PARTNER
Alpenstrasse 14
Postfach 4627
6304 Zug (CH)

(54) Method and token for registering users of a public-key infrastuture and registration system

(57) The method allows to register user in a public-key infrastructure based on credentials, including biometric data, such as data related to a fingerprint, presented to an authority (100) of the public-key infrastructure, comprising the steps of connecting a token (10), comprising a processor (2), an interface device (3) and a memory device (5), containing a private-key (51) and a public-key (52) for the user of the token (10) and a private-key (53) issued by the authority (100); reading biometric data (58) of the user, such as data derived from a fingerprint, by a biometric input device (1; 31); signing the biometric data (58) with the private-key (53) issued by the authority (100); sending a certification request, containing the public-key (52), signed biometric data (58) and additional credentials of the user, to the authority (100); verifying and registering the received data by the authority (100); storing the biometric data (58) in a database (104); returning a corresponding certificate (520) and storing the certificate (520) in the token. After registration the token is a secure element of the public-key infrastructure allowing to encrypt messages and securely sign messages, with digital signatures, on which a third party can rely on. In case of fraud biometric data taken from an unauthorised user can be stored in a database and later legally used as evidence.

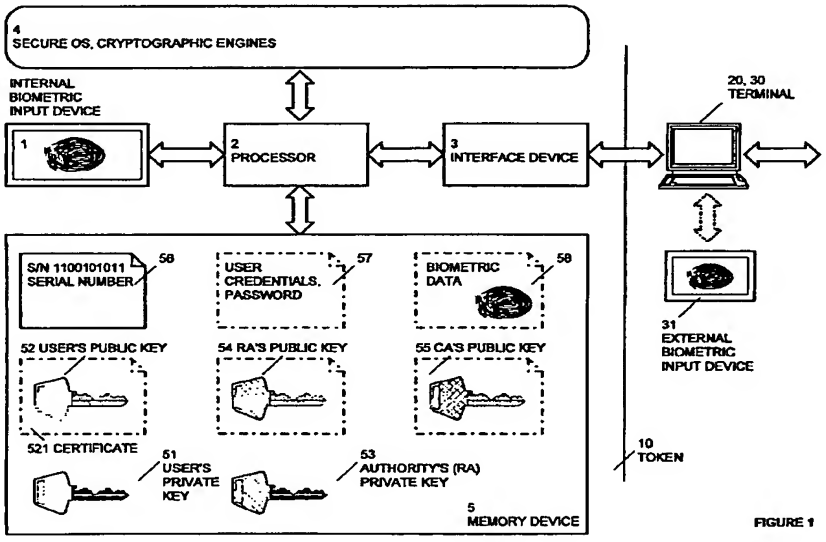

FIGURE 1

EP 1 263 164 A1

Description

[0001] The present invention relates to a method, a token and a registration system for registering users of a public-key infrastructure according to claim 1, 12 and 20 respectively.

[0002] The present invention relates in particular to a method for reliably registering users at an authority of the public-key infrastructure in such a way that third parties can trust the issued certificates.

[0003] More particularly the present invention relates to a method for performing said registration with a token, which is capable of processing biometric data.

BACKGROUND OF THE INVENTION

[0004] The emergence of the World Wide Web access to the Internet has been accompanied by recent focus on financial transaction vulnerabilities, crypto system weaknesses and privacy issues. Fortunately, technological developments also made a variety of controls available for computer security including tokens, biometric verifiers, encryption, authentication and digital signature techniques using preferably asymmetric public-key methods (see [1], Richard C. Dorf, THE ELECTRICAL ENGINEERING HANDBOOK, 2nd Edition, CRC-Press, Boca Raton 1997, chapter 97, pages 2221-2234 and [7], A. Menezes, P. van Oorschot, S. Vanstone, HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC-Press, Boca Raton 1997, chapter 1).

[0005] The basic security services to be provided are secrecy, authentication (assurance of sender identity to recipient), and digital signatures (authentication plus assurance to sender and third parties that the signature had not been created by the recipient). Also of importance is the notion of integrity which means preventing interference in the information conveying/storing process.

[0006] Almost all cryptosystems involve publicly known transformations of information, based on one or more keys, at least one of which being kept secret. The public-key cryptosystem disclosed 1976 by Diffie and Hellman is based on two keys, a private-key and a public-key, owned by users of this system.

[0007] As described in [2], U.S. Patent document No. 4,405,829 the public-key cryptosystem provides enciphered communication between arbitrary pairs of people, without the necessity of their agreeing on an enciphering key beforehand. The system of Diffie and Hellman, extended was extended by Tahar El Gamal (see [6]) to provide a method for creating a recognizable, unforgeable, document-dependent, digitised signature for a document whose authenticity the signer cannot later deny.

[0008] The RSA cryptosystem (named after R.L. Rivest, A. Shamir and L.M. Adleman which in [2] are mentioned as inventors) is the most widely used public-key cryptosystem. RSA is a commutative transformation which allows the private-key and the corresponding public-key to be used interchangeably as encryption or decryption keys, thus providing secrecy and authenticity on a secure channel between two parties A and B with no need for additional keys (see [1], pages 2225-2226).

[0009] Since, given only one key of an asymmetric key pair, it is practically infeasible to determine the other key, an owner A of a key pair may publish his public-key so that anyone can use this public-key to encrypt a message that only A can decipher with his private-key.

[0010] As described in [3], Marc Branchaud, A SURVEY OF PUBLIC-KEY INFRASTRUCTURES, Department of Computer Science, Mc Gill University, Montreal 1997, page 5, computing with public-key ciphers takes much longer than encoding the same message with a secret-key system. This has led to the practice of encrypting messages with a secret-key system such as DES and then encoding the secret-key with a public-key system such as RSA. In this case the public-key system securely transports the secret-key. In case that a message is sent secretly from A to B then, besides a secret-key, which is used optionally, only the key pair of B is used.

[0011] The described public-key system also allows owner A to sign a message to be sent to B with a digital signature. In this case the key pair of A is used. A encrypts the message or a corresponding hash of the message with his private-key which, on the other side of the transmission channel can be decrypted by B using A's public key. One key pair can therefore be used to receive an encrypted message or to send a digitally signed message.

[0012] B (and any third parties), who can decrypt with A's public-key a message signed by A, can therefore trust that A has signed the message as far as B can trust that the selected public-key truly belongs to A.

[0013] In order to ensure that public-keys can systematically be published and truly relate to the persons A, B, ... indicated by attached public-key values, registration and certification authorities (RA, CA) have been introduced to certify the relationship between a given key and a claimed identity.

[0014] According to [3], page 10, a public-key infrastructure, in its most simple form, is a system for publishing public-key values used in public-key cryptography. There are basic operations, namely registration, certification and validation, which are common to all public-key infrastructures.

[0015] Certification is the means by which registered public-key values, and information pertaining to those values, are published. A basic certificate therefore contains at least the public-key of the concerned subject, subject identification information, and identification information of the certifying authority.

[0016] The certificate is encrypted by the certification authority with the certification authority's private-key and can be decrypted with the publicly known public-key of the certification authority. In other words a certificate

is therefore an encyrypted message issued by the certification authority declaring that the therein contained public-key relates to the enclosed subject identification information.

[0017] As described in [3], pages 19-21, authentication is a service provided by a public-key infrastructure. When a certifying authority certifies an entity and a user then validates that certification, the entity is said to have been authenticated.

[0018] The degree to which a user can trust the certificate's information and it's validity is a measure of the strength of the authentication.

[0019] [4], U.S. Patent document NO. 6,202,151 B1 describes a biometric certification system and method which implements an end-to-end security mechanism binding the biometric identification of the certificate applicants with their digital certificate. The binding is achieved by including biometric measurements in the certificate itself.

[0020] Prior to use of the disclosed biometric certification system and method, the biometric database is built using a registration process in which individuals are required to provide proof of identity. Once the registration authority is satisfied with such proof, the identification information is entered into the biometric certification management system and biometric measurements are then taken concurrently using at least one biometric input device. Such stored biometric measurements form the pre-stored biometric data in the biometric database which corresponds to the pre-registered individuals who have undergone the registration process.

[0021] Accordingly, pre-registered individuals may be properly authenticated, while unregistered individuals are rejected.

[0022] As mentioned in [4], column 5 the user identification data ID may typically contain 50 bits or less. Biometric information, which will be part of the biometric certificate, may require a large amount of memory storage of up to 4 MB. The end-to-end security mechanism described in [4] handles therefore with each transaction large amounts of data which for authentication must be transferred to a biometric certification management system where the received biometric data are extracted and compared with stored biometric data resulting in a high workload for each transaction.

[0023] The process of implementing and handling the certification system described in [4] involves therefore the use of considerable resources.

[0024] Users can also be authenticated through something possessed such as a token or a smart card. Tokens are, as described in [1], pages 2228-2229, hand-carried devices that are normally intended to increase password security by assuring that passwords are used only once, thereby reducing the vulnerability to password compromise. Tokens may contain internally an algorithm, which either works in synchronisation with an identical algorithm in a host computer or which transforms an input derived from a computer prompt into a password that matches the computer-transformed result. In a public-key infrastructure a token containing a private-key may used to sign a message as described above.

[0025] The degree of authentication of a user by means of a token is however in many cases not strong enough. A person, to which the token had been assigned, may, rightfully or not, deny at a later stage that the token actually belongs to them or that the token is no longer in their possession.

[0026] It would therefore be desirable to improve the described public-key infrastructures. It would be desirable in particular to improve registration and authentication methods in public-key infrastructures thereby increasing the reliability of the system while keeping time and costs required for registration, authentication and processing at a low level. It would be desirable to provide a method allowing to register certificate applicants, using a token, at an authority of a public-key infrastructure in such a way that third parties can trust the certificate issued for said certificate applicant. It would also be desirable to create a token, which is capable of processing biometric data taken from its certificate applicant.

SUMMARY OF THE INVENTION

[0027] The above and other objects of the present invention are achieved by a method, a token and a registration system for registering users of a public-key infrastructure according to claim 1, 12 and 20 respectively.

[0028] The inventive method allows users to register by means of a token or another secure device at an authority, preferably the registration authority of a public-key infrastructure based on credentials, including signed biometric data presented to said authority.

[0029] The biometric data are signed by means of a private key issued individually for example by the registration authority automatically for each token, making the token itself part of the registration authority.

[0030] In addition to signing the biometric data with the private key of the registration authority the data can further be signed with the user's private key contained in the token.

[0031] The token therefore comprises a functionality of a registration authority which significantly increases trust into the inventive system compared to known solutions.

[0032] After registration the token is a secure element of the public-key infrastructure allowing the holder/user of the token to decrypt encrypted messages sent to them and to securely sign messages, with digital signatures, that can be relied on by a third party.

[0033] According to the present invention the token comprises a processor, a memory device, an operating system and an interface device designed for exchanging data with a terminal which is capable to access the network of the public-key infrastructure. The memory

device contains, included in a certificate, a private-key and a public-key for the user of the token and a private-key issued preferably by the registration authority which is used to sign and preferably encrypt biometric data read from an internal or external biometric input device.

[0034] The token is capable of storing a certificate which has been issued preferably by a certification authority of the public-key infrastructure based upon a certification request originating from the token.

[0035] To register a person for issuing a certificate is a difficult process, given the apparently contradictory requirements of, on the one hand, an inexpensive and convenient registration process and, on the other hand, strong mutual identification and authentication of the person and the certification authority, secure mutual exchange of their respective public keys and the secure storage of the person's private key on a token.

[0036] The inventive method allows the generated key pair contained in the token to be strongly bound to its owner/user since the authority of the public-key infrastructure, by means of the provided private-key issued by the registration authority, signs the biometric data read immediately at the users side.

[0037] The registration process is therefore considerably simplified for all parties.

[0038] Since the binding of the token to the user is strong and security of the public-key infrastructure is sufficient, even for high level transactions, there is no need to include the biometric data in the certificate issued for the token i.e. the user. Transactions are therefore not burdened with additional data to be transferred and processed for authentication purposes. Biometric data are therefore not included in each transaction since the existence of the biometric data does not increase the cryptographic security of the public key infrastructure as whole.

[0039] The authority of the public-key infrastructure, which preferably consists of a registration authority, a certification authority and a key and certificate management unit, issues preferably for each token an individual key-pair, a private-key used for signing the biometric data and a public-key which is used for decrypting signed messages at the site of the registration authority or, in case that it is also stored in the token, as well for encrypting messages, such as the certification request, sent to the registration authority.

[0040] Instead of or in addition to the public-key of the registration authority, the certificate of the certification authority or the certification path that validates the certification authority's certificate may be stored in the token so that messages sent to the authority of the public-key infrastructure may be encrypted..

[0041] In a preferred embodiment of the invention the biometric input device is integrated in the token which facilitates secure and trustworthy registration procedures and further usage of the token.

[0042] In order to prevent usage of the token by non-authorised persons, additional measures may be taken. The memory device of the token may store a password, biometric data or a hash of the biometric data. Access to the private- and public-key is then only granted in case that the entered biometric data and/or the password match the stored values. In the case that the entered biometric data does not match the stored values, then the entered biometric data originating from an unauthorised user could also be stored as evidence for legal prosecution.

[0043] Biometric data in preferred embodiments of the invention is however protected and never leaves the token unencrypted. Only in case of settling a fraud dispute will biometric data, either stored in the token or in the database of the authority, be disclosed for the purposes of expediting legal prosecution.

[0044] In order to optimise security and to facilitate handling of the tokens, the key pair for the user, the private-key and the public-key are preferably generated within the token. Critical data, in particular the data of the user, and said private keys are preferably not accessible by external devices.

[0045] The invention on the one hand therefore allows to strongly authenticate a user i.e. a partner in a transaction and on the other hand protects the user against misuse of the token without adding noteworthy burden onto the users or operators of the public-key infrastructure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0046] Some of the objects and advantages of the present invention have been stated, others will appear when the following description is considered together with the accompanying drawings, in which:

Figure 1 shows the schematic of an inventive token and

Figure 2 shows a public key infrastructure with inventive tokens implemented in a network such as the Internet.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0047] The inventive token shown in figure 1 is designed for registering users at an authority 100 of a public-key infrastructure which normally comprises a registration authority 101, in charge of registering new users of the public-key infrastructure, a certification authority 102, in charge of issuing certificates based on approved user's certification requests and a key and certificate management unit 103, handling and validating certificates and keys. Issued and revoked certificates of the users as well as the certificate of the certification authority 102 are published in a directory 104 to which said authorities 101, 102, 103 and users have access.

[0048] After the registration has been completed, the

token 10 with it's private key and certificate then builds part of the public-key infrastructure, which allows its user to perform transactions over a network 200 such as the Internet.

[0049] An inventive token 10, which according to [1], pages 2228-2229, is a hand-carried device, comprised in its basic embodiment of a processor 2, a memory device 5, an operating system 4 including at least one cryptographic engine and an interface device 3, preferably a USB (universal serial bus) interface, designed for exchanging data with a terminal 20, 30 which is capable to access the network services 200 of the public-key infrastructure. The memory device 5 contains a private-key 51 and a public-key 52 for a user of the token 10 and a private-key 53 issued by the authority 100, preferably by the registration authority 101.

[0050] In order to optimise security and facilitate handling the user's key pair, the private-key 51 and the public-key 52 are preferably generated within the token 10. In this case the private-key 51, before or after the registration procedures, will never be available outside the token 10.

[0051] Tokens 10 are therefore normally initialised and issued by the authority 100, preferably the registration authority 101.

[0052] The token 10 comprises an internal biometric input device 1 or can be connected via the terminal 30 to an external biometric input device 32. Biometric data read during the registration procedures by the internal or external biometric input device 1, 31 is processed in the token 10 thereby signing at least said biometric data or a derivate, for example a hash generated thereof, by means of the private-key 53 issued by the authority 100, preferably the registration authority 101.

[0053] Signed biometric data, the user's public key 52 and possibly additional credentials of the user, which have been transferred through the terminal 20, 30 to the token 10 are entered into a certification request assembled preferably based on the Standard PKCS#10 (see [5], PKCS#10 Standard, Certification Request Syntax Standard, RSA Laboratories, May 2000) and sent to the authority 100, preferably the registration authority 101.

[0054] The registration authority 101 verifies and registers the received data and stores the user's credentials including the biometric data in the database 104. The authority 100, preferably the certification authority 102 then issues based upon the approved certification request a certificate 521 containing the user's public key 52 which then, possibly accompanied by the certification authority's 102 own certificate, is returned to the token 10 and stored therein.

[0055] The above mentioned PKCS#10 standard describes options for protecting the contents of the certification request. According to the present invention, biometric data sent as part of a PKCS #10 certificate request will be protected for integrity, non-repudiation and privacy.

[0056] In a preferred embodiment of the invention, besides the private-key 53, the public-key 54 of the registration authority 101 and/or the public-key 55 of the certification authority 102 are stored in the memory device 5 of the token 10 so that the certification request or data contained therein can be encrypted with one of these public-key 54, 55 before they are sent to the registration authority 101.

[0057] In the case where the encryption of the certification request is performed with the certification authority's 102 public-key 55, then the message is decrypted by the private-key of the certification authority 102. In case that the encryption of the certification request is performed with the registration authority's 101 public-key 54, then the message is decrypted by the private-key 53 of the registration authority 101.

[0058] In order to optimise security the authority 100, preferably the registration authority 101, issues for each token 10 an individual key-pair, a public-key 54 and a private-key 53, which is used for signing the biometric data.

[0059] In order to facilitate the retrieval of the required keys 53, 54 at the registration authority 101 the certification request is preferably accompanied by a serial number 56, which is stored in the memory device 5 of the token 10. The key pair 53, 54 issued for a token 10 is therefore preferably linked to its serial number.

[0060] Since none of the keys for signing the biometric data 58 are publicly available, the authority 100, preferably the registration authority 101, may use an asymmetric key pair 53, 54 or a symmetric key pair for signing the biometric data 58. In case that a symmetric key is enclosed in the token 10, then the registration authority 101 my find the corresponding symmetric key by means of the serial number of the token 10. In the same manner instead of a symmetric key a shared password, a password contained in the token 10 and a corresponding password stored at the registration authority 101, could be used for signing the biometric data 58. However as described above the use of an asymmetrical key pair is preferred compared to the use of a symmetrical key or a shared password, since sharing symmetrical keys or passwords always involves additional risks.

[0061] After the registration process has been completed and a certificate 521 has been issued the token is strongly linked to its user, so that based on the provided reliability and trust, high level transactions can be executed, since the user of the token can reliably be authenticated.

[0062] In order to protect the user against losses in case of theft of the token, biometric data 58 or a derivative such as a hash thereof or a password is preferably stored in the memory device 5. The password and further credentials of the user are stored in block 57 of the memory device 5 shown in figure 1. Access to the functions of the token 10 is then provided only when a password entered and/or biometric data read by the internal or external biometric input device 1, 31 matches the stored values.

[0063] The comparison of said data is preferably done within the token 10. The system is therefore not burdened with access procedures during which relatively large amounts of data need to be transferred.

[0064] It is however possible that biometric data read from the current user of the token 10 are transferred to the authority 100 for verification purposes. In the case that delivered values do not match stored values, data access is denied. The biometric data could optionally be stored in the database 104 or in the token (when used offline),for legal prosecution of non-authorised users of the token 10.

[0065] Figure 2 shows a public key infrastructure with inventive tokens 10a, 10b, 10c implemented in a network 200 such as the Internet. The authority 100 shown consists of a registration authority 101, a certification authority, a key and certificate management unit 103 and a database 104 containing the directory of the public key infrastructure. The users of tokens 10a and 10b, which contain integrated biometric data input devices 1 are connected to terminals 20 through which transactions can be carried out with users other terminals 20, 40.

[0066] Figure 2 further shows a registration system 35 which is preferably installed in places where tokens 10 can be obtained. In particular registration procedures with tokens 10 which do not contain an integrated biometric data input device 1 are performed with a registration system 35 which comprises a terminal 30 and a at least one device 31 capable of reading biometric data of a user. The registration system 35 may be connected to a scanner for reading fingerprints, to a camera or to a voice recorder.

[0067] Although the present invention has been described in detail with reference to preferred embodiments, persons having ordinary skill in the art will appreciate that various modifications and different implementations may be made without departing from the spirit and scope of the invention.

REFERENCES :

[0068]

[1] Richard C. Dorf, THE ELECTRICAL ENGINEERING HANDBOOK, 2nd Edition, CRC-Press, Boca Raton 1997

[2] U.S. Patent document No. 4,405,829

[3] Marc Branchaud, A SURVEY OF PUBLIC-KEY INFRASTRUCTURES, Department of Computer Science, Mc Gill University, Montreal 1997

[4] U.S. Patent document NO. 6,202,151 B1

[5] PKCS#10 Standard, Certification Request Syntax Standard, RSA Laboratories May 2000 (available under http://www.rsasecurity.com/rsalabs/pkcs/index.html)

[6] Taher El Gamal, A PUBLIC KEY CRYPTOSYSTEM AND SIGNATURE SYSTEM BASED ON DISCRETE LOGARITHMS, IEEE Transactions on Information Theory, 31(4), 474-481, 1985

[7] A. Menezes, P. van Oorschot, S. Vanstone, HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC-Press, Boca Raton 1997

Claims

1. Method for registering users of a public-key infrastructure based on credentials of a user, including biometric data such as data related to a fingerprint, presented to an authority (100) of the public-key infrastructure, comprising the steps of

   a) connecting a token (10),
   which comprises a processor (2), an interface device (3) and a memory device (5), containing a private-key (51) and a public-key (52) for the user of the token (10) and a private-key (53) issued by the authority (100);
   to a terminal (20, 30) capable to access the network (200) of the public-key infrastructure,

   b1) reading biometric data (58) of the user, such as data derived from a finger print of the user, by a biometric input device (1; 31);

   b2) signing the biometric data (58) with a key of an asymmetric or symmetric key pair or by means of a shared password issued by the authority (100);

   b3) sending a certification request, containing the public-key (52), signed biometric data (58) and additional credentials of the user, to the authority (100);

   c1) verifying and registering the received data by the authority (100);

   c2) storing the biometric data (58) in a database (104);

   c3) returning a corresponding certificate (520) and

   d) storing the certificate (520) in the token.

2. Method according to claim 1 comprising the steps

of double signing the biometric data with said key of an asymmetric or symmetric key pair or by means of a shared password and the user's private key (51).

3. Method according to claim 1 or 2, with a serial number of the token being stored in the memory device (5), which, included in the certification request, is sent to the authority (100) which, based on said serial number, retrieves the symmetric or asymmetric key or the password matching the key or password used for signing the biometric data (58) in order to decrypt the signed message.

4. Method according to claim 1, 2 or 3 for a public-key infrastructure with an authority (100), consisting of a registration authority (101), a certification authority (102) and a key and certificate management unit (103), comprising the steps of issuing for each token (10) an individual symmetric or asymmetric key-pair, a first key stored in the token (10) for signing the biometric data (58) and a second key (54) stored at the registration authority (101).

5. Method according to claim 1, 2, 3 or 4 with the public-key (54; 55) of the registration authority (101) and or the certification authority (102) being stored in the token (10), comprising the steps of encrypting at least the part of the certification request containing the biometric data with one of said public-keys (54; 55) before sending it and decrypting the received certification request by the registration authority (101) with the corresponding private-key (53, ...) .

6. Method according to one of the claims 1-5 with the biometric input device (31) being integrated in the token (10) comprising the steps of pressing a finger onto the token (10) while biometric data (58) is read.

7. Method according to one of the claims 1-6 comprising the steps of storing the biometric data (58) or a hash of the biometric data (58) in the memory device (5) and/or storing a password in the memory device (5).

8. Method according to one of the claims 1 to 7 comprising the steps of comparing a password entered with the password stored in the token (10) and/or reading biometric data from the user and comparing biometric data read with biometric data (58) stored in the token (10) or in the database (104) of the authority (100) and providing access to the system in case that the compared data match and/or storing mismatched data as proof for legal prosecution of a non-authorised user of the token 10.

9. Method according to one of the claims 1 to 8 comprising the steps of generating the key pair for the user, the private-key (51) and the public-key (52) within the token (10).

10. Method according to one of the claims 1 to 9 comprising the steps of performing transactions defined by the authority of the public-key infrastructure while using the registered token (10).

11. Method according to one of the claims 1 to 10 comprising the steps of keeping the user's data, particularly the biometric data, private except for cases of fraud.

12. Token (10) designed for registering users at an authority (100) of a public-key infrastructure particularly according to the method of claim 1, comprising a processor (2), a memory device (5), an operating system (4) and an interface device (3) designed for exchanging data with a terminal (20, 30) which is capable to access the network (200) of the public-key infrastructure, **characterised in that**

a) the memory device (5) contains a private-key (51) and a public-key (52) for a user of the token (10) and a private-key (53) issued by the authority (100);

b) the token (10) is capable of processing biometric data (58) read and transferred from an internal or external biometric input device (31);

c) the token (10) is capable of signing the read biometric data (58) with a key of an asymmetric or symmetric key pair or by means of a shared password issued by the authority (100);

d) the token (10) is capable of storing a certificate (520) which has been issued by the authority (100) based upon a certification request originating from the token (10).

13. Token (10) according to claim 12 capable of signing the read biometric data (58) with the key of the asymmetric or symmetric key pair or by means of a shared password and the user's private key (51).

14. Token (10) according to claim 12 or 13, with a serial number of the token being stored in the memory device (5).

15. Token (10) according to claim 12, 13 or 14 for a public-key infrastructure with an authority (100), consisting of a registration authority (101), a certification authority (102) and a key and certificate management unit (103), comprising an individual key of a symmetric or asymmetric key-pair or a shared password for signing the biometric data (58) and a

public-key (55) issued by the registration authority (101) or the certification authority (102) for encrypting the certification request sent to the authority (100).

16. Token (10) according to one of the claims 12-15 with the biometric input device (1) being integrated in the token (10).

17. Token (10) according to one of the claims 12-16 designed to store the read biometric data (58) or a hash of the biometric data (58) in the memory device (5) and/or storing a password in the memory device (5).

18. Token (10) according to one of the claims 12-17 capable to compare a password entered with the password stored in the token (10) and/or capable of reading biometric data from the user and comparing biometric data read with biometric data (58) stored in the token (10) providing access to the system in case that the compared data match.

19. Token (10) according to one of the claims 12-18 capable to generating the key pair for the user, the private-key (51) and the public-key (52), within the token (10).

20. Registration system (35) providing access to a token (10) according to one of the claims 12-19 with a terminal(30) designed to exchange data with the network (200) of the public-key infrastructure, with a connected token (10) and with at least one biometric input device (31) capable of reading biometric data, preferably as data related to a fingerprint, the retina, the face and/or the voice of a user which biometric data is transferable via the terminal (30) to the token (10) for processing.

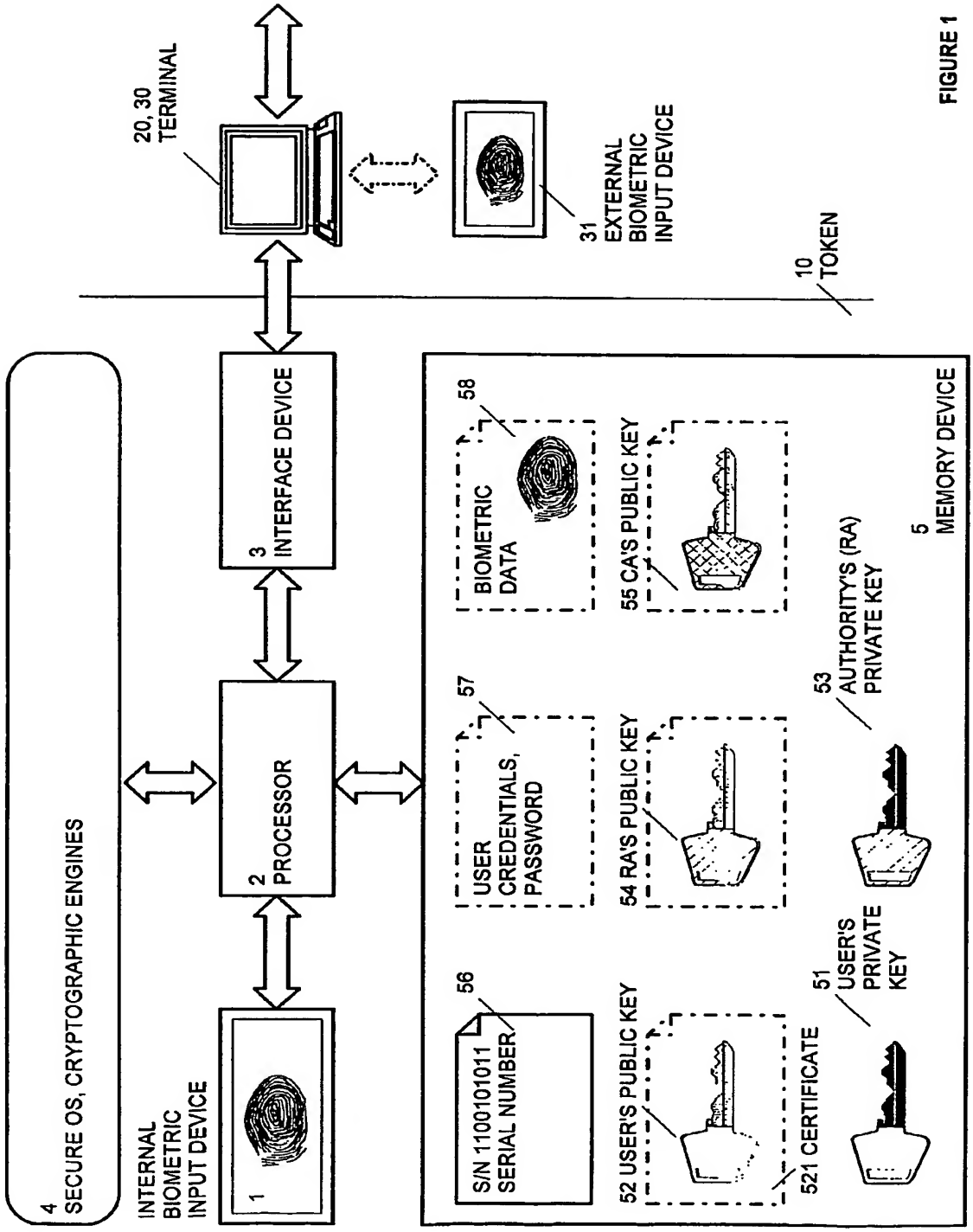
20, 30
TERMINAL
31
EXTERNAL
BIOMETRIC
INPUT DEVICE
10
TOKEN
4
SECURE OS, CRYPTOGRAPHIC ENGINES
INTERNAL
BIOMETRIC
INPUT DEVICE
1
2
PROCESSOR
3
INTERFACE DEVICE
58
BIOMETRIC
DATA
55 CA'S PUBLIC KEY
57
USER
CREDENTIALS,
PASSWORD
54 RA'S PUBLIC KEY
53
AUTHORITY'S (RA)
PRIVATE KEY
5
MEMORY DEVICE
56
S/N 1100101011
SERIAL NUMBER
52 USER'S PUBLIC KEY
521 CERTIFICATE
51
USER'S
PRIVATE
KEY

FIGURE 1

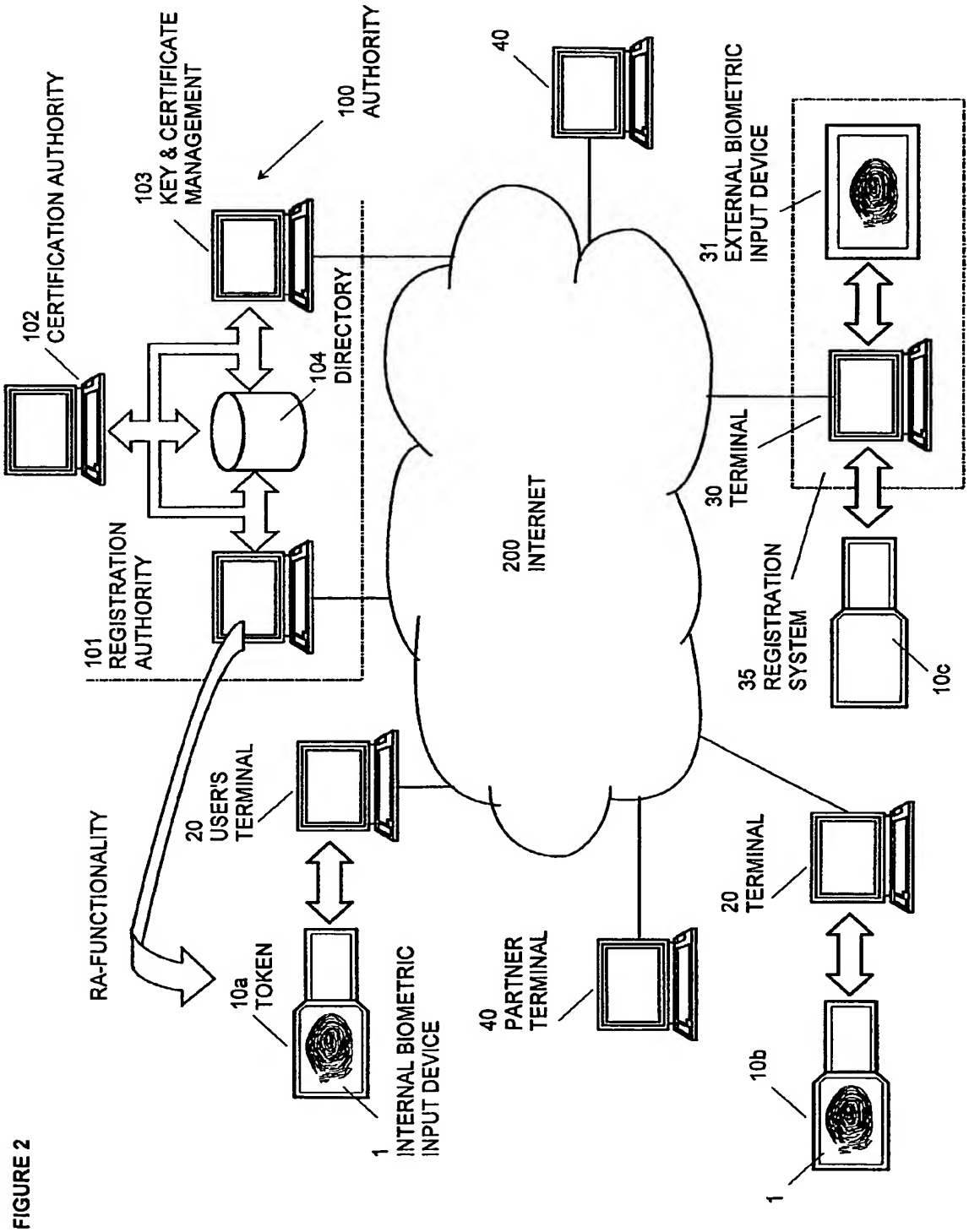
102
CERTIFICATION AUTHORITY
103
KEY & CERTIFICATE
MANAGEMENT
100
AUTHORITY
104
DIRECTORY
101
REGISTRATION
AUTHORITY
RA-FUNCTIONALITY
20
USER'S
TERMINAL
10a
TOKEN
1
INTERNAL BIOMETRIC
INPUT DEVICE
200
INTERNET
40
40
PARTNER
TERMINAL
31
EXTERNAL BIOMETRIC
INPUT DEVICE
30
TERMINAL
35
REGISTRATION
SYSTEM
10c
20
TERMINAL
10b
1

FIGURE 2

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 81 0637

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	WO 98 50875 A (GTE GOVERNMENT SYST ;GTE SERVICE CORP (US)) 12 November 1998 (1998-11-12) * page 7, line 4 - line 19 * * page 8, line 6 - line 16 * * page 9, line 9 - line 27 * * claim 16 * * figure 3 *	1-20	H04L9/32
Y	EP 0 999 528 A (ELSDALE LIMITED) 10 May 2000 (2000-05-10) * column 2, line 6 * * column 4, line 22 - column 5, line 23 * * column 8, line 39 * * paragraphs '0006!,'0022!,'0023!,'0039!,'0041! *	1-20	
Y	R. FOURNIER, T. KAMIONEK: "The Cryptographic Smart Card: An integrated Solution" RSASECURITY WEB SEMINARE, 'Online! 25 April 2001 (2001-04-25), pages 1-30, XP002213544 Retrieved from the Internet: <URL:www.rsasecurity.com> 'retrieved on 2002-09-05! * page 4 - page 8 * * page 13 - page 23 * * page 13 - page 23 *	1-20	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G07C H04L H04K B60R G07F G06F
A	US 6 189 096 B1 (HAVERTY RAND) 13 February 2001 (2001-02-13) * column 3, line 42 - column 4, line 5 * * column 9, line 42 - column 10, line 34 * * column 15, line 46 - line 60 * * figure 10 *	1-20	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	25 September 2002	Bec, T

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 81 0637

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	US 5 280 527 A (FAST NORMAN ET AL) 18 January 1994 (1994-01-18) * column 3, line 37 - column 4, line 9 * * column 4, line 37 - line 64 * * column 5, line 33 - column 6, line 5 * * figures 1-3 *	1-20	
A	POLEMI D: "TTPs and biometrics for securing the payment of telemedical services" FUTURE GENERATIONS COMPUTER SYSTEMS, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 15, no. 2, 11 March 1999 (1999-03-11), pages 265-276, XP004222994 ISSN: 0167-739X * paragraph '0005! *	12-19	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	25 September 2002	Bec, T

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 81 0637

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

25-09-2002

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
WO 9850875	A	12-11-1998	AU	7484898 A	27-11-1998
			BR	9808737 A	16-01-2001
			CN	1274448 T	22-11-2000
			EP	0980559 A2	23-02-2000
			JP	2002501700 T	15-01-2002
			US	6105010 A	15-08-2000
			US	6202151 B1	13-03-2001
			US	6208746 B1	27-03-2001
			US	6310966 B1	30-10-2001
			WO	9850875 A2	12-11-1998
EP 0999528	A	10-05-2000	DE	19851074 A1	11-05-2000
			EP	0999528 A2	10-05-2000
US 6189096	B1	13-02-2001	AU	3624599 A	23-11-1999
			CA	2330958 A1	11-11-1999
			CN	1299545 T	13-06-2001
			EP	1076953 A1	21-02-2001
			WO	9957846 A1	11-11-1999
			JP	2002514842 T	21-05-2002
US 5280527	A	18-01-1994	CA	2105404 A1	03-03-1995

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82